

Security overview

Last updated 30 October 2026.

This page explains, in plain terms, how Signature HQ protects your organisation and what it can and cannot access. It should be read with our Privacy Policy and Terms. Signature HQ is run by Leadica Limited in New Zealand. We do not currently hold SOC 2 or ISO 27001 certification.

1. What Signature HQ can access

- **Directory details** for people in your Microsoft 365 or Google Workspace: name, email address, whether the account is enabled, and, if you switch on Directory details, job title, department, phone numbers, office location and company name.
- **Microsoft 365**: nothing in your mailboxes. Signature HQ holds no Exchange permission or role. The Outlook add-in inserts the approved signature while a person writes an email.
- **Google Workspace**: read and set the signature on the included user's Gmail send-as address, and read the staff list. No other Gmail operation is allowed; we never read mail.
- Nothing else in your mailboxes.

2. What Signature HQ cannot access

- We do not read, send, store or scan email messages, attachments, calendars, contacts or files.
- We do not hold your users' passwords.
- The Outlook add-in only asks Microsoft who the signed-in person is (their basic profile), then fetches that person's approved signature and inserts it. It uses only Outlook's signature features and the type of message being written (new, reply or forward). It never reads the message body, subject, recipients, sender or attachments, and its diagnostic log never records message content. Automated tests check this.

3. Microsoft 365 permissions

Signature HQ uses one Microsoft app, **Signature HQ Add-in**. It has:

Its Application (client) ID is **9b2d3cf9-ca09-455e-bfea-01ce8c6b7a0b**. Check this ID when approving the app in Microsoft Entra.

- **Microsoft Graph User.Read.All** (application): read the user directory to match people to staff and, if you switch on Directory details, their job title and phone numbers.
- **Microsoft Graph Organization.Read.All** (application): confirm which organisation and verified domains approved Signature HQ.
- **Delegated User.Read, openid and profile**, plus our own **access_as_user** scope: lets the Outlook add-in confirm who the signed-in person is.

It has **no Exchange permission and no Exchange administrator role**, and cannot read, send or change email or mailbox settings. The app signs in to Microsoft with a certificate only; it has no client secret.

4. Google Workspace permissions

Domain-wide delegation is limited to two scopes:

- **gmail.settings.basic**: read and set only the signature on the target user's send-as address.

- **admin.directory.user.readonly**: read the staff list and verify the Super Admin.

Each domain-wide token carries only the scope needed for that call, never both. Directory calls impersonate only the verified Super Admin; signature calls impersonate only the target mailbox. Every token and data call rechecks the active verified domain and organisation/platform pause. An endpoint allow-list blocks forwarding, filters, IMAP/POP, vacation settings, labels and messages, even though Google's basic settings scope itself is broader. Per-mailbox Google OAuth is disabled.

Before first deployment we privately save the original send-as signature. Removal restores it by default, with an explicit Clear option. The backup is deleted after successful removal or organisation closure. Token mints are audited without tokens. Deployments run in batches of at most 25 with a per-organisation lock, cooldown and bounded retry backoff for Google rate limits or temporary failures.

5. Ownership checks before connecting

Before any connection is used, we check that the Microsoft or Google administrator who approved Signature HQ belongs to the organisation and domain being connected. Connections are tied to a single Signature HQ organisation and cannot be reused by another customer.

6. Data we store

- Organisation and brand settings, templates, banners and images you upload.
- Staff signature details (name, title, phones, links and similar).
- Mailbox matching and rollout status, deployment history and audit records.
- Signature link click counts (time, link, destination, browser type and referring page). We do not record the clicker's email or IP address.
- Billing details are held by Stripe. Card details are never stored on our systems.

The homepage signature preview runs in your browser and is not saved.

7. Subprocessors

- **Supabase** (through Lovable Cloud): database, sign-in and file storage
- **Cloudflare**: hosting, content delivery and security
- **Lovable**: application platform, service email delivery, and AI features in some admin tools (processed by OpenAI or Google through Lovable's AI service)
- **Firecrawl**: fetching public branding from a website you give us during setup
- **Stripe**: payments, subscriptions and invoices

8. Encryption

- All traffic to the app, the Outlook add-in and hosted signature images uses HTTPS (TLS).
- Data is encrypted at rest by our database and storage provider.
- Connection credentials are kept on the server and are never sent to browsers.

9. Sign-in and two-factor authentication

- Leadica platform staff (Owner, App Admin and Support roles) must set up and verify an authenticator before using the app after sign-in.

- Organisation admins must use an authenticator app once their organisation has a connected Microsoft 365 or Google Workspace account. There is no grace period: setup or verification is a full-screen sign-in step that cannot be dismissed.
- Organisations can require two-factor sign-in for all staff. Signing in with Microsoft or Google counts as two-factor for editors and staff, because your own identity provider applies its sign-in rules.
- Support staff have read-only access and cannot deploy, remove, connect, edit or change roles.
- Sensitive actions may require a fresh authenticator code during the session. An Owner can reset another user's authenticator after checking their identity; recovery is audited. Contact support@leadica.io if you lose your authenticator.

10. Audit logging and change notifications

We record connections, deployments, removals, rollout inclusion changes, role and access changes, delivery pauses, allowed-link changes, image replacements, sign-in email change requests and two-factor recovery. Records show who made the change and when.

Organisation admins get an hourly email summary of changes to templates, staff signatures, banners, buttons, links and images, including changes made by Leadica staff, with a link to review them.

11. Protection against tampering

- **Allowed link domains:** every link in a signature must point to one of the organisation's allowed domains. A signature with any other link cannot be approved or delivered.
- **Delivery pause:** organisation admins can stop all signature delivery for their organisation straight away. Leadica Owners have a platform-wide emergency pause. Both are audited.
- **Image history:** replacing a hosted image keeps a private backup and a version record so it can be restored.
- **Re-confirming identity:** sensitive actions (connecting or disconnecting, changing delivery, approving signatures, changing allowed links, pausing delivery, replacing images and changing roles) need an authenticator code entered in the last 10 minutes. This applies to Leadica staff and to admins of organisations with a connected Microsoft 365 or Google Workspace account.

12. Rate limits and abuse protection

Public forms, the Outlook add-in signature service and diagnostics are rate limited. Public forms also use hidden spam checks. Sign-ups require email confirmation.

13. Image-only hosted assets

Hosted signature images are checked when uploaded and served only as images. Uploads must be real image files. Private files cannot be served through public image links, and the image host cannot be used to serve web pages or scripts.

Only active admins and editors of the asset's organisation, or Leadica platform Owners and App Admins, can upload or replace its images. Support and viewers cannot write files, and anonymous uploads are blocked. Uploads are restricted to the authorised organisation's image paths and validated PNG, JPEG, GIF or WebP files. Replacements go through the server's private-backup and version-history checks; direct uploads cannot bypass them.

14. Sessions and browser security

- Leadica platform sessions end after 1 hour of inactivity and 12 hours after sign-in.

- Platform staff and organisation admins get an email when their account signs in from a new device.
- The app sends browser security headers that stop it being embedded in other websites. The Outlook add-in pages use a strict content policy that only allows Signature HQ and Microsoft sign-in and Office addresses.

15. Revoking access

You can stop Signature HQ at any time:

- **Microsoft 365:** remove the Outlook add-in in Integrated apps, then delete the Signature HQ Add-in Enterprise application in Microsoft Entra. If you connected before October 2026, also delete the older Signature HQ Enterprise application and any Exchange Recipient Administrator assignment it was given.
- **Google Workspace:** restore original signatures (or explicitly clear them) before disconnecting. Disconnect in Signature HQ immediately blocks all Google calls; no domain-wide tokens are cached. Then go to admin.google.com > Security > Access and data control > API controls > Manage Domain Wide Delegation, find the Signature HQ client ID, click Delete and confirm.
- **In Signature HQ:** disconnect the integration and remove central signatures if you want them cleared.

Signatures already installed stay in place until removed.

16. Retention

Customer data is kept while the organisation is active. Some records are deleted automatically: Outlook add-in diagnostics after 30 days, signature link clicks after 13 months and security audit records after 2 years. Logs never include passwords, access tokens or connection credentials. After cancellation, you can request an export for 30 days, and we then delete the data within 90 days, apart from backups on their normal cycle and records we must keep by law. Full details are in our Privacy Policy.

17. Reporting a security issue

Please email hello@leadica.io with details of any suspected vulnerability. We will acknowledge your report, keep you updated, and ask that you give us reasonable time to fix the issue before sharing it. Please do not access other customers' data or disrupt the Service while testing.